UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-cv-954

FARHAD AZIMA,

Plaintiffs,

v.

NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC.,

Defendants.

COMPLAINT

Plaintiff, Farhad Azima, by and through his undersigned counsel, files this Complaint against Nicholas Del Rosso ("Del Rosso") and Vital Management Services Inc. ("Vital"; collectively, "Defendants"), and alleges as follows:

INTRODUCTION

1. Defendants Del Rosso and Vital oversaw and directed the hacking of Plaintiff Farhad Azima. Defendants stole Azima's computer data, including emails and trade secrets. The stolen data was then published online and used by Defendants and others, on behalf of the Ras Al Khaimah Investment Authority ("RAKIA"), in an attempt to ruin Azima's reputation and damage him financially. Upon information and belief, Defendants were engaged and paid by Dechert LLP, which represented RAKIA in a dispute with Azima.

2. RAKIA, the state investment entity for the government of Ras Al Khaimah, hired individuals and companies, directly and through Dechert LLP, to investigate Azima,

hack his computers, steal his private data, and weaponize that data in an attempt to ruin Azima. Those individuals and companies included Stuart Page in the United Kingdom and the Defendants in the United States. Defendant Vital was hired by Dechert LLP through partner Neil Gerrard on behalf of RAKIA, and Defendants then hired CyberRoot Risk Advisory Private Limited ("CyberRoot") to provide the technical support necessary to hack Azima. CyberRoot is a company based out of Gurgaon, India that engages in illegal hacking.

3. BellTroX Info Tech Services ("BellTroX") assisted CyberRoot in hacking Azima. BellTroX is a hacking company based in New Delhi, India. According to a June 9, 2020, press report by Thomson Reuters, BellTroX was involved in "one of the largest spy-for-hire operations ever exposed," helping clients spy on more than 10,000 email accounts over a period of seven years. On February 11, 2015, the founder and owner of BellTroX, Sumit Gupta, was indicted by the United States Department of Justice in the Northern District of California for hacking. Gupta remains at large.

4. In its investigation of 'hack-for-hire' organizations (including BellTroX), Thomson Reuters reviewed a cache of data revealing "tens of thousands of malicious messages designed to trick victims into giving up their passwords" – phishing and spear phishing emails – that BellTroX distributed between 2013 and 2020. Upon information and belief, the data cache revealed that email accounts belonging to Azima and his associates were among the accounts targeted by the BellTrox/CyberRoot phishing operation.

5. Defendants paid CyberRoot more than $1 million for the hacking of Azima and the dissemination of his stolen data.

6. At the direction of Del Rosso and Vital, CyberRoot sent Azima phishing and spear-phishing emails, and successfully induced Azima to unwittingly provide them with passwords for his accounts. The successful hack gave CyberRoot persistent access to Azima's computers and email accounts, and CyberRoot obtained real time access to Azima's emails. CyberRoot disclosed Azima's stolen data on internet blog sites they created. These blog sites contained links to BitTorrent sites and We Transfer sites, set up by CyberRoot, that contained at least some of the data Defendants and CyberRoot stole from Azima. The work done by CyberRoot, assisted by Bell TroX, was done at the direction of the Defendants and others.

7. Defendants hacked Azima because they were hired to do so on behalf of RAKIA by Gerrard and Dechert LLP. Dechert LLP represented RAKIA in a dispute with Azima, and Gerrard wanted Azima's stolen data to use in a suit to be brought by RAKIA against Azima in England. Page, Del Rosso, Gerrard, and RAKIA's manager James Buchanan created a false evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents. RAKIA brought the lawsuit against Azima using the hacked material. The hacking was a defense raised by Azima, as well as forming the basis for a counterclaim by Azima.

8. The English court ruled that RAKIA, Page, and others had lied about how they obtained Azima's stolen data. Del Rosso gave a sworn witness statement in the U.K. suit, denying any knowledge of how the stolen emails were obtained. That witness statement was false. Del Rosso gave live, sworn testimony during the trial. That testimony was false as well. RAKIA's lawyers, including Dechert LLP, had also asserted (in formal correspondence, witness evidence and pleadings signed by those lawyers) that RAKIA had innocently discovered the materials on the internet. Those assertions were also false, given the Judge's ruling.

9. As a result of the conduct of Del Rosso, Vital, and their co-conspirators, Azima has suffered significant financial and reputational damage.

PARTIES

10. Plaintiff Farhad Azima is a U.S. citizen who resides and works in Kansas City, Missouri. He is a successful businessman who has owned and operated multiple aviation-related companies. Azima's businesses engage in interstate and foreign commerce. All of Azima's computers and servers were and are located in the United States.

11. Defendant Nicholas Del Rosso is the owner and sole employee of his company, Defendant Vital Management Services Inc. ("Vital"). Vital purports to provide investigative services, but it is not licensed as a private investigator in North Carolina. Vital is located at 1340 Environ Way, Chapel Hill, North Carolina, 27517, and Del Rosso lives at 318 Lystra Preserve Drive, Chapel Hill, North Carolina 27517.

12. Defendant Del Rosso is the president and owner of Vital, and he is one of two shareholders of Vital, along with his wife.

FACTS

13. Dechert LLP and partner Neil Gerrard hired Del Rosso and Vital to "investigate assets potentially stolen from the Government of Ras Al Khaimah ("RAK")." Throughout the course of his work for Dechert LLP, which lasted from at least August 2014 until at least 2019, Del Rosso was hired by Dechert LLP and Gerrard. Del Rosso communicated with lawyers from Dechert LLP on a "very regular basis." Del Rosso hired Chris Swecker, a North Carolina-based lawyer, to assist Defendants in their work for Gerrard and Dechert LLP.

The Hacking of Azima at Del Rosso's Direction

14. Starting in early 2015, Gerrard, Page, Buchanan, and others agreed to attack Azima. The agreement is evidenced by a redacted internal "Project Update" report dated March 26, 2015, presented by Page to the Ruler of RAK and provided to Buchanan and others, as well as numerous emails between Gerrard, Buchanan, and their associates, some of which discussed the plan to "target," "attack," and "go after" Azima using "another channel." Based on these emails, an English court concluded that the desire to attack Azima in the summer of 2015 "is clear." The Project Update report claimed Azima was part of a "US team" to publicize human rights abuses by RAK and Gerrard. The report stated that "[t]he campaign is not public yet, so we will be able to gather intelligence on their progress in order to monitor their activities and attempt to contain or ruin their plans." Gerrard admitted to reading this report.

15. Gerrard hired Del Rosso and Vital. Upon information and belief, Del Rosso was hired to target Azima and to obtain Azima's emails and confidential data, as well as for other purposes; and Page was retained to assist in the targeting of Azima, which upon information and belief included hacking Azima.

16. Del Rosso hired the Indian hacking firm CyberRoot to provide the technical expertise to attempt to lure Azima into providing his login data, so that Defendants and their co-conspirators could have persistent access to Azima's accounts and computers. At least five employees of CyberRoot, including one of the company's directors, Vibhor Sharma, hacked Azima pursuant to Del Rosso's instructions. CyberRoot was assisted by BellTroX, which permitted CyberRoot to use BellTroX's infrastructure, including its server, to conduct the hacking. This work was done at the direction of the Defendants and others. CyberRoot and BellTroX share common employees. One such employee is Preeti Thapiyal, whose LinkedIn page lists his work as including the creation of "undetectable phishing Payloads."

17. CyberRoot, assisted by BellTroX, attempted to gain access to Azima's computers and accounts through phishing and spear-phishing emails. They sent Azima phishing emails to harvest his credentials and gain access to his email accounts and computers. Azima complied, and unwittingly enabled CyberRoot's hackers to gain access to Azima's email accounts and computers. The breach of Azima's computer systems gave CyberRoot covert and persistent access to Azima's email accounts and computers.

18. Del Rosso, Vital, CyberRoot, and other co-conspirators, including Dechert LLP, Gerrard, and Page, obtained numerous confidential and protected trade secrets belonging to Azima and his companies, including but not limited to privileged and confidential legal communications and advice and confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan.

The Disclosure of Azima's Stolen Data at Del Rosso's Direction

19. Acting at Defendants' direction, CyberRoot created, uploaded, and transmitted multiple unauthorized copies of Azima's data. Upon information and belief, at least some of that data was provided to Del Rosso, who was located in North Carolina.

20. In late July 2016, Gerrard met with Azima and threatened him. Within days of Gerrard's meeting with Azima, CyberRoot, which was assisted by BellTroX, created blog sites on or about August 7, 2016, accusing Azima of fraud. During this same period, Del Rosso made significant payments to CyberRoot for their efforts.

21. The websites contained links to BitTorrent sites that Dechert LLP later admitted contained large quantities of Azima's stolen data. These BitTorrent links were posted by users named anjames and an_james. The usernames anjames and an_james are usernames associated with Sharma at CyberRoot. CyberRoot also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data.

22. CyberRoot posted the data on the internet to create the misimpression that the data CyberRoot and Defendants stole from Azima were available to anyone who used the internet. CyberRoot created BitTorrent links that contained Azima's stolen data and those

links were posted on the blog sites alleging fraud by Azima. Page, Del Rosso, Gerrard, and an Israeli journalist, Majdi Halabi, created a false story and evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents after being alerted to it by Halabi.

23. In fact, the data on the BitTorrent links were not accessible to the public because the "seeders"[1] necessary for the data to be downloaded were not available. Dechert LLP, and others acting at their direction, are the only persons or entities known to have obtained the data from the BitTorrent sites.

24. In May and June 2018, the blog sites were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data.

25. CyberRoot regularly used WeTransfer links to transfer data to Vital. CyberRoot set up the WeTransfer account using the email account an_james@protonmail.ch.

26. In June 2019, the links on the blog sites were modified to include new WeTransfer links containing some of Azima's stolen data. These links, as with all the links to copies of Azima's stolen data, were not authorized by Azima.

27. Defendants were engaged by Dechert LLP on behalf of RAKIA. Upon information and belief, Defendants were paid by Dechert LLP, directly or indirectly, for their work.

[1] A torrent seeder is a user who owns the file being made available online through the torrent system. Without a seeder, a file cannot be downloaded.

28. Upon information and belief, Dechert LLP paid Defendants more than $1 million.

29. Defendants paid CyberRoot more than $1 million.

30. Those payments were for CyberRoot's hacking services and the distribution of Azima's stolen data.

31. At least some of the payments made by Vital were sent to CyberRoot's bank, Kotak Mahindra Bank.

32. Substantial payments were made to CyberRoot around the time that Azima's stolen data was published online in August and September 2016.

Lawsuit Against Azima and False Testimony About Discovery of Azima's Data

33. In September 2016, Dechert LLP partner David Hughes, on RAKIA's behalf, threatened to file a lawsuit in the U.K. against Azima and provided Azima's counsel with some of the emails that Defendants and CyberRoot stole from Azima. RAKIA, represented by Dechert LLP, sued Azima in England in September 2016 repeatedly relying on the data that Defendants stole from Azima.

34. Prior to and during the January 2020 trial in the U.K., Dechert LLP and RAKIA repeatedly changed their stories about how Azima's stolen data was obtained. The English court ruled that the story put forward by RAKIA and others on their behalf about how they discovered the stolen data was false. Specifically, the court said that the story told by Page, Halabi, and others of innocent discovery of Azima's stolen data was "not true," involved "unexplained contradictions, inconsistencies, and implausible elements," and "was both

internally inconsistent and inconsistent with the contemporaneous documents."[2] The English court said that "the true facts" about how Dechert LLP and others obtained Azima's stolen data still "have not been disclosed," despite them being required to do so. The untrue story of innocent discovery was advanced by RAKIA's agents. Former Dechert LLP partner Hughes signed a statement of truth for RAKIA advancing the story of innocent discovery. Others, including Gerrard, Buchanan, and Page, put forward witness statements and testimony that supported the story the court found to be untrue.

35. Del Rosso was an important part of RAKIA's false story of "innocent discovery" by Page of Azima's stolen data. For example, Gerrard and Del Rosso exchanged a series of emails on August 15 and 16, 2016, in which Gerrard purported to "break the news" of the discovery of the hacked material on websites. But other evidence showed that Del Rosso was aware of these websites at least a week earlier. The emails of August 15 and 16, 2016, between Gerrard and Del Rosso were clearly an attempt to lay a false "paper trail" of discovery.

36. In his witness statement, Del Rosso hid his engagement of CyberRoot and denied any involvement in the hacking. Because of Del Rosso's concealment of the true facts, of which he had knowledge, Azima did not learn of the role played by Del Rosso and Vital until recently.

[2] *Ras Al Khaimah Investment Authority v. Farhad Azima*, [2020] EWHC 1327 (Ch).

JURISDICTION

37. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331. Some of Azima's claims arise under federal law, including the Wiretap Act (Counts 1 and 2) and misappropriation of trade secrets under the Defend Trade Secrets Act and the Economic Espionage Act (Count 3).

38. The Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over Azima's other claims, since those other claims relate to the federal statutory claims in this action and form part of the same case or controversy under Article III of the United States Constitution.

39. Additionally, this Court has diversity subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Azima and Defendants are from different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

40. The Court's jurisdiction over defendants comports with due process. The Court has personal jurisdiction over Defendants Del Rosso and Vital, who are domiciled or have their principal place of business in North Carolina. Del Rosso works at Vital in North Carolina and lives at 318 Lystra Preserve Drive, Chapel Hill, North Carolina 27517. Vital is based in North Carolina and is located at 1340 Environ Way, Chapel Hill, North Carolina, 27517.

VENUE

41. Venue is proper under 18 U.S.C. § 1965(a) because the Defendants transact their affairs in this Judicial District. Defendants Del Rosso and Vital both transact their

affairs in Chapel Hill, North Carolina, with Azima's causes of action arising out of those North Carolina transactions.

42. Venue is also proper under 28 U.S.C. § 1391(b)(2) because this is a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred. Defendants conspired with others and coordinated their illegal campaign to hack Azima and publish his stolen data from their principal place of business in Chapel Hill, North Carolina.

43. Venue is also proper under 28 U.S.C. § 1391(b)(3) because this judicial district has personal jurisdiction over all defendants.

COUNT ONE (All Defendants)

I. Disclosure of Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(c) and 2520)

44. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

45. It is a violation of 18 U.S.C. § 2511(c) for any person to "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication."

46. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

47. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce."

48. In violation of 18 U.S.C. § 2511(1)(c), Defendants Del Rosso and Vital intentionally disclosed wire and electronic communications of Azima knowing and/or having reason to know that the information was obtained through interception.

49. Defendants Del Rosso and Vital directed CyberRoot to intentionally disclose large quantities of Azima's intercepted data by instructing that the data be posted on BitTorrent and WeTransfer. Links to those BitTorrent and WeTransfer sites were added to the blog sites that CyberRoot created. CyberRoot worked with BellTroX and at the direction of the Defendants to conduct the hacking and post the intercepted data. The BitTorrent and WeTransfer sites were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. CyberRoot also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data. The links were updated as recently as 2019.

50. The intercepted data included, among other things, business and personal electronic communications between Azima and others across the United States and around the world.

51. Defendants Del Rosso and Vital caused CyberRoot to hack Azima's computers and email accounts. The hack gave CyberRoot persistent access to Azima's computers and email accounts.

52. Defendants Del Rosso and Vital knew or had reason to know that the information published on the BitTorrent and WeTransfer sites was obtained through interception because Del Rosso and Vital gave the instructions to CyberRoot to intercept Azima's data and paid CyberRoot more than $1 million to conduct the hack and publish the stolen data. Defendants Del Rosso and Vital also knew or had reason to know that the information was obtained through interception because, among other reasons discussed above, it included large quantities of privileged, private, financially sensitive and trade secrets data, including private email communications, banking documentation, and business plans, including confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan.

53. As a result of the disclosure of Azima's intercepted data, Azima suffered damages. Since at least June 2018, the stolen data has continued to be publicly available on WeTransfer through links that were posted to the blog sites created by CyberRoot, resulting in more than $75,000 of statutory damages under 18 U.S.C. § 2520(c)(2)(B), and further monetary damages in an amount to be proven at trial. Upon information and belief, Defendants Del Rosso and Vital have made significant profits from the disclosure of Azima's data, having been paid large sums of money to disclose the stolen data to damage Azima. As a result of the continued disclosure of Azima's stolen data, Azima has suffered,

and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT TWO (All Defendants)

II. Conspiracy to Disclose and Use Intercepted Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(d) and 2520, 18 U.S.C. § 371)

54. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

55. Defendants Del Rosso and Vital willfully, intentionally, and knowingly agreed and conspired with CyberRoot, Dechert LLP, Page, and others to disclose Azima's intercepted data in violation of 18 U.S.C. §§ 2511 and 2520. Among other things, Defendants Del Rosso and Vital agreed and conspired to intercept Azima's data through a phishing and spear-phishing campaign resulting in the hackers obtaining persistent access to Azima's computers and email accounts. Defendants Del Rosso and Vital paid more than $1 million for the interception of Azima's data. Defendants Del Rosso and Vital also agreed and conspired to disclose the intercepted data by instructing CyberRoot to publish the data on blog sites that were created by CyberRoot. CyberRoot used BitTorrent and WeTransfer to send the stolen data to Defendants Del Rosso and Vital as well as other co-conspirators.

56. The BitTorrent and WeTransfer links were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. Defendants also

used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data.

57. Defendants Del Rosso and Vital, with full knowledge that they were engaged in wrongful actions, took steps in furtherance of the conspiracy, including paying more than $1 million to the company that conducted the hacking, and later covering up the hacking through a story that the English court found to be false.

58. Azima has been injured and has suffered monetary damages as a result of Defendants' conspiratorial actions in an amount to be proven at trial. As a result of the Defendant's conspiracy to disclose and use Azima's intercepted data, Azima has suffered, and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT THREE (All Defendants)

III. Misappropriation of Trade Secrets, 18 U.S.C. §§ 1831, 1832, 1836

59. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

60. Federal law creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

61. Federal law imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). See § 1832(a)(5).

62. Federal law also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." 18 U.S.C. § 1831(a)(1).

63. Federal law imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). See § 1831(a)(5).

64. "An owner of a trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1).

65. Azima's email accounts and computer systems stored trade secrets, including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships. These trade secrets are substantially valuable to Azima, in excess of $75,000, as will be proven at trial.

66. Azima stored trade secrets that were used in interstate and foreign commerce. Azima has taken and continues to take reasonable measures to keep this information secret.

For example, Azima has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

67. Azima's trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

68. Azima's trade secrets have significant value, resulting from substantial investment of time and resources.

69. Azima has made, and continues to make, efforts that are reasonable under the circumstances to maintain the secrecy of his trade secrets.

70. Defendants Del Rosso and Vital, along with CyberRoot, Dechert LLP, Page, and others, unlawfully conspired to take, appropriate, and obtain Azima's trade secrets without authorization, by means of a cyberattack against him. Defendants Del Rosso and Vital and their co-conspirators knew that Azima's email accounts contained trade secrets and intended to steal them in order to harm Azima.

71. Defendants Del Rosso and Vital improperly disclosed and misappropriated Azima's trade secrets without consent or authorization when they instructed CyberRoot to hack Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs created by CyberRoot.

72. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Azima has suffered damages, which include, but are not limited to, loss of business goodwill, loss in the value of his trade secrets and

confidential business information, and harm to Azima's business, in an amount to be proven at trial. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I). Defendants' acts of misappropriation have affected interstate commerce.

73. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Defendants Del Rosso and Vital have unjustly benefited from their possession of Azima's trade secrets. Upon information and belief, Defendants Del Rosso and Vital, who were engaged by Dechert LLP, were paid substantial sums of money by Dechert LLP to conspire to steal and misappropriate Azima's trade secrets. Del Rosso and Vital in turn paid CyberRoot more than $1 million.

74. Defendants' conduct was willful and malicious.

COUNT FOUR (All Defendants)

IV. Computer Trespass (N.C. Gen. Stat. § 14-458)

75. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

76. In violation of N.C. Gen. Stat § 14-458, Defendants Del Rosso and Vital directly and/or through their agents knowingly and without authorization or reasonable grounds used Azima's computer and computer network with the intent to make or cause to be made unauthorized copies of Plaintiff's computer data.

77. Defendants had no right, authority, or permission to access or use Plaintiff's computer data or computer network.

78. Defendants Del Rosso and Vital conspired with others to use Azima's computer and computer network without authorization to make copies of Plaintiff's trade secrets, confidential business information, and personal information and communications that would provide Defendants and their co-conspirators leverage over Plaintiff.

79. Defendants Del Rosso and Vital instructed CyberRoot to hack Azima's computer and computer network and aided and abetted the hacking of Azima's computer data and computer network. At the direction of Defendants Del Rosso and Vital, CyberRoot, which worked with BellTroX, carried out the hack on Azima and gained access to Azima's computer and computer network. The breach of Azima's computer systems gave CyberRoot persistent access to Azima's email accounts and computers. Thus CyberRoot, acting at the direction of Defendants Del Rosso and Vital and others, regularly used Azima's computer and computer networks to make unauthorized copies of Azima's computer data, and Defendants Del Rosso and Vital caused these unauthorized copies to be made. Defendants Del Rosso and Vital paid CyberRoot more than $1 million for their hacking services.

COUNT FIVE (All Defendants)

V. Conversion (North Carolina Common Law)

80. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

81. Plaintiff was the lawful owner of his computer data and computer network, and was entitled to immediate and exclusive possession of his computer data and computer network.

82. Defendants directly and/or through their agents and co-conspirators, knowingly and without authorization or reasonable grounds, wrongfully possessed and converted computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

83. Under North Carolina law, conversion occurs when a defendant wrongfully possesses or converts property under the ownership of the Plaintiff.

84. Defendants conspired to wrongfully obtain and exercise possession of Plaintiff's computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

85. As discussed in more detail above, Defendants Del Rosso and Vital instructed CyberRoot to hack Azima and make unauthorized copies of Azima's computer data. At the direction of Defendants Del Rosso and Vital, CyberRoot successfully hacked Azima and converted Plaintiff's computer data by obtaining and utilizing persistent access to Azima's email accounts and computer systems. Thus CyberRoot, acting at the direction of Defendants Del Rosso and Vital and other co-conspirators, regularly accessed Azima's computer and computer networks to make unauthorized copies of Azima's computer data, and Defendants Del Rosso and Vital caused these unauthorized copies to be made.

Defendants Del Rosso and Vital paid CyberRoot more than $1 million for their hacking services.

COUNT SIX (All Defendants)

VI. Identity Theft (N.C. Gen. Stat. § 14-113.20 and § 1-539.2(c))

86. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

87. Defendants directly and/or through their agents and co-conspirators knowingly and without authorization or reasonable grounds, obtained, possessed, and used identifying information of Plaintiff with the intent to fraudulently represent that Defendants were the Plaintiff for the purposes of obtaining materials of value, benefit, and advantage.

88. Pursuant to N.C. Gen. Stat. § 14-113.20, "identifying information" is defined to include "passwords;" "electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;" and "any other numbers or information that can be used to access a person's financial resources."

89. Defendants conspired with CyberRoot, Dechert LLP, Page, and others to obtain, possess, and use Plaintiff's identifying information – including electronic mail passwords – for the purposes of stealing and misappropriating trade secrets, confidential business information, and personal information and communications that would provide Defendants and their co-conspirators leverage over Plaintiff.

90. At the direction of Del Rosso, Vital, and others, CyberRoot sent Azima phishing emails asking him to reset his password. Azima complied, and unwittingly

permitted CyberRoot's hackers to gain access to Azima's email accounts and computers. The persistent access to Azima's email accounts and computers allowed CyberRoot, at the direction of Defendants Del Rosso and Vital, to use Azima's email addresses and passwords to obtain substantial quantities of Azima's private data, including trade secrets, confidential business information, and personal information and communications.

COUNT SEVEN (All Defendants)

VII. Publication of Personal Information (N.C. Gen. Stat. § 75-66)

91. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

92. Defendants knowingly broadcast or published personal information of Azima on the internet with actual knowledge that Azima objected to any such disclosure and without Azima's consent or knowledge.

93. Defendants published Azima's private information on blog sites hosting WeTransfer links in May and June of 2018, and again in June of 2019.

94. This personal information included, among others, checking account numbers, passwords, and other numbers and information that can be used to access Azima's financial resources.

95. Among other documents, Defendants published financial transaction records, spreadsheets, business records, and banking information, all of which were and are marked confidential.

96. Defendants' publication of Azima's personal information on the internet despite Azima's objection and without Azima's consent or knowledge directly and proximately caused actual injury to Plaintiff.

97. Defendants and their co-conspirators were not permitted, authorized, or required by any federal, State, or local law, regulation, or ordinance to access, collect, use, or release Azima's sensitive and confidential personal information.

98. At the direction of Del Rosso, Vital, and others, CyberRoot created blog sites accusing Azima of fraud. The blog sites contained links to BitTorrent sites that Dechert LLP later admitted contained large quantities of Azima's stolen data. These BitTorrent links were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. CyberRoot also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data. In May and June 2018, the blog sites were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data CyberRoot regularly used WeTransfer links to transfer data to Vital. CyberRoot set up the WeTransfer account using the email account an_james@protonmail.ch.

99. During this same period, Del Rosso made significant payments to CyberRoot for their efforts.

100. Azima is entitled to damages for each of Defendants' unlawful acts of publication of personal information in accordance with N.C. Gen. Stat. § 1-539.2(c).

COUNT EIGHT (All Defendants)

VIII. Violation of Trade Secrets Protection Act (N.C. Gen. Stat. § 66-153 *et seq*.)

101. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

102. Azima's email accounts and computer systems contained business or technical information, formulas, patterns, programs, devices, compilations of information, methods, techniques, or processes. This information included highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships. This information constituted trade secrets under Chapter 66 of the North Carolina General Statutes.

103. Azima derived independent actual or potential commercial value from these trade secrets not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from their disclosure or use.

104. Azima has undertaken and continues to undertake reasonable efforts under the circumstances to maintain the secrecy of his trade secrets. For example, Plaintiff has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

105. Azima's trade secrets are substantially valuable to Plaintiff, in excess of $75,000, as will be proven at trial.

106. Azima kept trade secrets that were used in interstate and foreign commerce.

107. Azima's trade secrets have significant value, resulting from substantial investment of time and resources. If known to Azima's competitors, Plaintiff's trade secrets would be of value to those competitors.

108. Azima's trade secrets included, among others, confidential internal price lists and confidential spreadsheets connected to contracts with the United States government to supply troops in Afghanistan.

109. Defendants Del Rosso and Vital, along with CyberRoot, Dechert LLP, Page, and others, unlawfully conspired to acquire, disclose, or use Azima's trade secrets without express or implied authority or consent by means of a cyberattack against Azima. Defendants Del Rosso and Vital and their co-conspirators knew that Azima's email accounts and computer systems contained trade secrets and intended to steal them in order to harm Azima. Defendants did not arrive at Azima's trade secrets by means of independent development, reverse engineering, or by obtaining them from a person or entity with a right to disclose any of the trade secrets.

110. Defendants Del Rosso and Vital improperly acquired, disclosed, or used Azima's trade secrets without consent or authorization when they instructed CyberRoot to hack Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs created by CyberRoot.

111. Defendants' conduct in acquiring, disclosing, or using Azima's trade secrets was willful and malicious and part of a deliberate, clandestine strategy and conspiracy to injure Azima.

112. Azima discovered that Defendants misappropriated his trade secrets earlier this year.

113. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Azima has suffered damages, including but are not limited to loss of business goodwill, loss in the value of his trade secrets and confidential business information, and harm to Azima's business, in an amount to be proven at trial. Defendants' acts of misappropriation have affected interstate commerce.

114. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Defendants Del Rosso and Vital have unjustly benefited from their possession of Azima's trade secrets. Upon information and belief, Defendants Del Rosso and Vital, who were engaged by Dechert LLP, were paid substantial sums of money by Dechert LLP to conspire to misappropriate Azima's trade secrets.

115. Del Rosso and Vital paid CyberRoot more than $1 million to conspire to misappropriate Azima's trade secrets.

116. Defendants' conduct in misappropriating Azima's trade secrets as described above directly and proximately caused actual injury to Azima.

117. Because Defendants' conduct was willful and malicious, Azima is entitled to punitive damages pursuant to N.C. Gen. Stat. § 66-154(c).

118. Because Defendants' conduct was willful and malicious, Azima is entitled to reasonable attorney's fees under N.C. Gen. Stat. § 66-154(d).

COUNT NINE (All Defendants)

IX. Unfair and Deceptive Trade Practices (N.C. Gen. Stat. § 75-1.1)

119. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

120. Defendants' conduct in sending Azima phishing and spear phishing emails in an effort to access and misappropriate his emails, computers, communications, confidential information, personal information, trade secrets, and other data constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

121. Defendants' conduct in accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data without his consent or knowledge constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

122. Defendants' conduct in publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

123. Defendants committed conduct in or affecting commerce by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other

data without his consent or knowledge, and (3) publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

124. Defendants committed conduct that was unfair and deceptive by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data, and (3) publishing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

125. Defendants' conduct in committing the unfair and deceptive acts or practices as described above was willful and malicious and part of a deliberate, clandestine strategy and conspiracy to injure Azima.

126. Defendants' conduct in committing the unfair and deceptive acts or practices as described above directly and proximately caused actual injury to Azima.

127. Plaintiff discovered that Defendants committed unfair and deceptive acts or practices that injured him on or about August 28, 2020 following an investigation.

128. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1, Plaintiff's damages should be trebled pursuant to N.C. Gen. Stat. § 75-16.

129. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1 and Defendants willfully and maliciously engaged

in that conduct, Plaintiff is entitled to recover reasonable attorney's fees pursuant to N.C. Gen. Stat. § 75-16.1.

COUNT TEN (All Defendants)

X. Civil Conspiracy (North Carolina Common Law)

130. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

131. Defendants and their co-conspirators CyberRoot, Dechert LLP, and others, knowingly and without authorization or reasonable grounds, wrongfully entered into an agreement to commit unlawful acts resulting in injury to Azima by conspirators pursuant to a common scheme of stealing Azima's confidential information to use against him.

132. Under North Carolina law, a civil conspiracy occurs when there is an agreement between two or more individuals to do an unlawful act or to do a lawful act in an unlawful way, resulting in injury to a plaintiff inflicted by one or more of the conspirators pursuant to a common scheme.

133. Under this agreement, Defendants directed that CyberRoot send phishing emails to induce Azima to reveal his credentials. Defendants would then use Azima's credentials to gain access to Azima's confidential information and copy the information for widespread publication. Defendants paid CyberRoot more than $1 million for these actions. Upon information and belief, Defendants were contracted and paid by Dechert LLP, on behalf of RAKIA, to conduct the hacking.

134. Because of Defendants' successful and unlawful phishing campaign against Azima, Azima had confidential information publicly exposed, suffered harm to business relationships, and suffered misappropriation of numerous trade secrets.

135. Defendants, CyberRoot, Dechert LLP, and Page engaged in this conspiracy pursuant to a common scheme of damaging Azima and tarnishing his reputation. Defendants are thus liable for the unlawful and tortious acts of all of the co-conspirators.

COUNT ELEVEN (All Defendants)

XI. Invasion of Privacy – Offensive Intrusion Upon Seclusion

136. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

137. Defendants intruded upon Azima's privacy by invading his solitude, seclusion, private affairs and personal concerns.

138. Defendants invaded Azima's privacy intentionally because they knew that the hacking of Azima's email accounts and computer systems would intrude upon his privacy, or, at a minimum, Defendants acted with reckless indifference to the consequences of conspiring with Dechert LLP, CyberRoot, and other yet unknown co-conspirators to hack Azima's email accounts and computer systems.

139. Azima was and is highly offended by Defendants' intrusion upon his privacy, and any reasonable person would be highly offended under the same or similar circumstances. Azima reasonably expected that the highly confidential and sensitive

information, including confidential trade secrets, stored in his email accounts and computer systems would remain private.

PRAYER FOR RELIEF

On the basis of the foregoing, and such evidence as Plaintiff will present at trial, Plaintiff requests the entry of judgment in his favor and against Defendants on all counts of the Complaint and the award of the following relief:

1. Compensatory damages incurred by Azima as a result of the actions of Defendants, in an amount to be determined at trial.

2. Statutory damages, in an amount to be determined at trial, including treble damages and punitive damages.

3. A mandatory injunction requiring Defendants to remove and return of Azima's data from any computers, servers, or websites.

4. A prohibitory injunction obligating Defendants to refrain in the future from committing tortious acts against Plaintiff.

5. Pre-judgment and post-judgment interest in the amounts and at the rates provided by law.

6. Costs and expenses, including reasonable attorney's fees, incurred by Plaintiff in this action and as a result of the actions of Defendants alleged herein.

7. Such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff Farhad Azima respectfully requests a trial by jury of all issues so triable.

This, the 15th day of October, 2020.

Respectfully submitted,

WOMBLE BOND DICKINSON (US) LLP

/s/ Jonathon Townsend
Jonathon D. Townsend
North Carolina 51751
Christopher W. Jones
North Carolina Bar No. 27625
Ripley Rand
North Carolina Bar No. 22275
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: jonathon.townsend@wbd-us.com
ripley.rand@wbd-us.com
chris.jones@wbd-us.com

MILLER & CHEVALIER CHARTERED

/s/ Kirby D. Behre
Kirby D. Behre (*pro hac vice forthcoming*)
Brian Hill (*pro hac vice forthcoming*)
Tim O'Toole (*pro hac vice forthcoming*)
Ian Herbert (*pro hac vice forthcoming*)
Calvin Lee (*pro hac vice forthcoming*)
900 16th Street, NW
Washington, D.C. 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com

Counsel for Plaintiff